UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/769,173	01/30/2004	Sherman (Xuemin) Chen	15415US01	7811

23446   7590   03/13/2007
MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER
PALIWAL, YOGESH

ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	10/769,173	CHEN ET AL.
	Examiner	Art Unit	
	Yogesh Paliwal	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *1/30/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date *8/8/2005.*

4)☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

U.S. Patent and Trademark Office

PTOL-326 (Rev. 08-06)   Office Action Summary   Part of Paper No./Mail Date 20070305

DETAILED ACTION

Claim Rejections - 35 USC § 101

1.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The USPTO "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility" (Official Gazette notice of 22 November 2005), Annex IV, reads as follows:

> Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works and a compilation or mere arrangement of data.

> When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994) (claim to data structure stored on a computer readable medium that increases computer efficiency held statutory) and Warmerdam, 33 F.3d at 1360-61, 31 USPQ2d at 1759 (claim to computer having a specific data structure stored in memory held statutory product-by-process claim) with Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory).

> In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035.

Claims **11-20** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter as follows. Claims 11-20, define a *machine-readable storage* embodying functional descriptive material. However, claims do not define a computer-readable medium or memory and is thus non-statutory for that reason (i.e., "When functional descriptive material is recorded on some computer-

readable medium it becomes structurally and functionally interrelated to the medium

and will be statutory in most cases since use of technology permits the function of the

descriptive material to be realized" – Guidelines Annex IV). That is, the scope of the

presently claimed "machine readable storage" includes paper on which the program is

written, which is non-statutory. The examiner suggests amending the claim to embody

the program on "computer-readable medium" or equivalent in order to make the claim

statutory. Any amendment to the claim should be commensurate with its

corresponding disclosure.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-41 are rejected under 35 U.S.C. 102(b) as being anticipated by

Akiyama (US2002/0001386).

Regarding **Claim 1,** Akiyama discloses a method for secure key authentication,

the method comprising:

generating at a first location a digital signature of a secure key to obtain a

digitally signed secure key **(Paragraph 0112, lines 7-10, "the contract information**

shown in FIG. 5 except for the digital signature is sequentially encrypted for

respective blocks using the secret key, and the last block is used as a digital

signature.") *[It should be noted that, "contract information" contains the secret key, see*

at Fig. 5, "Work keys"]

and transmitting the digitally signed secure key from the first location **(Fig. 1,**

Numeral 102)

Regarding **Claim 2**, the rejection of claim 1 is incorporated and further Akiyama

discloses generating the digital signature from at least one of an asymmetric encryption

algorithm and a symmetric encryption algorithm **(Paragraph 0111, lines 9-10,**

"authenticates the digital signature using key information (secret key or public

key) stored in a digital signature")

Regarding **Claim 3**, the rejection of claim 1 is incorporated and further Akiyama

discloses encrypting the digitally signed secure key prior to transmission to obtain an

encrypted digitally signed key **(Fig. 7, "Enciphered contract information", also at**

Paragraph 0106, lines 5-8, "The individual control packet is comprised of an

information identifier, master key identifier, and encrypted contract information,

as shown in FIG. 7.") *[Each digitally signed contract information is encrypted using and*

master key]

Regarding **Claim 4**, the rejection of claim 3 is incorporated and further Akiyama

discloses the secure key comprises at least one of a master key, a work key and a

scrambling key. (*Fig. 5, "Work keys"*)

Regarding **Claim 5**, the rejection of claim 4 is incorporated and further Akiyama

discloses the receiving the digitally signed secure key at a second location (**Paragraph**

0110, lines 1-2, "Upon receiving an individual packet via the public telephone

network and modem 101...")

decrypting the digitally signed secure key to obtain a decrypted digitally signed

secure key (**Paragraph 0110, Lines 11-17, "If the master key identifier matches the**

master key, that master key is output from the master key storage 103 (step S4) to

decrypt contract information in the individual information packet")

Regarding **Claim 6**, the rejection of claim 5 is incorporated and further Akiyama

discloses if the secure key comprises a work key then a decrypted digitally signed

master key at the second location is utilized for decrypting an encrypted digitally signed

work key (**Paragraph 0110, Lines 11-17, "If the master key identifier matches the**

master key, that master key is output from the master key storage 103 (step S4) to

decrypt contract information in the individual information packet (step S5). Work

key information (pairs of work key identifiers and work keys and the like)

contained in the decrypted contract information is stored in a work key storage

105")

Regarding **Claim 7**, the rejection of claim 5 is incorporated and further Akiyama

discloses if the secure key comprises a scrambling key then a decrypted digitally signed

work key at the second location is utilized for decrypting an encrypted digitally signed

scrambling key **(Paragraph 0125, lines 9-14, "If the work key can be acquired,**

information of an encrypted section in the common control packet is decrypted

using the work key (step S44). A channel key Kch is acquired from the decrypted

information, and is stored in the channel key storage 118")

Regarding **Claim 8**, the rejection of claim 5 is incorporated and further Akiyama

discloses verifying authenticity of the digital signature of the digitally signed secure key

(Paragraph 0112, line 1-2, "digital signature authentication process")

Regarding **Claim 9**, the rejection of claim 8 is incorporated and further Akiyama

discloses verifying the authenticity of the digital signature utilizing at least one of an

asymmetric decryption algorithm and a symmetric decryption algorithm **(Paragraph**

0111, lines 7-11, "the contract information certifying device 107 certifies or

authenticates the digital signature using key information (secret key or public

key) stored in a digital signature authentication key storage 108")

Regarding **Claim 10**, the rejection of claim 8 is incorporated and further Akiyama

discloses determining whether to verify authenticity of the digital signature **(Paragraph**

0111, lines 6-8, "If the two IDs match, the contract information certifying device

107 certifies or authenticates the digital signature using key information")

Claims **11, 21 and 32** are "computer program" and "system" claims analogous to

"method" claim 1. Akiyama in the same reference discloses a system for performing

method of claim 1 [Broadcast receiver is depicted in figure 1 and Transmitter system is

depicted in figure 29]. Also, it should be noted that since Akiyama's system discloses

the hardware to perform the method of claim 1, therefore it would also have computer software that performs the method of claim 1. Claims 11, 21 and 32 are rejected under same rationale as the rejection of claim 1.

Claims **12, 22 and 33** are "computer program" and "system" claims analogous to "method" claim 2. Claims 12, 22 and 32 are rejected under same rationale as the rejection of claim 2.

Claims **13, 23 and 34** are "computer program" and "system" claims analogous to "method" claim 3. Claims 13, 23 and 34 are rejected under same rationale as the rejection of claim 3.

Claims **14, 24 and 35** are "computer program" and "system" claims analogous to "method" claim 4. Claims 14, 24 and 35 are rejected under same rationale as the rejection of claim 4.

Claims **15, 25 and 36** are "computer program" and "system" claims analogous to "method" claim 5. Claims 15, 25 and 36 are rejected under same rationale as the rejection of claim 5.

Claims **16, 26 and 37** are "computer program" and "system" claims analogous to "method" claim 6. Claims 16, 26 and 37 are rejected under same rationale as the rejection of claim 6.

Claims **17, 28 and 38** are "computer program" and "system" claims analogous to "method" claim 7. Claims 17, 28 and 38 are rejected under same rationale as the rejection of claim 7.

Claims **18, 28 and 39** are "computer program" and "system" claims analogous to "method" claim 8. Claims 18, 28 and 39 are rejected under same rationale as the rejection of claim 8.

Claims **19, 29 and 40** are "computer program" and "system" claims analogous to "method" claim 9. Claims 19, 29 and 40 are rejected under same rationale as the rejection of claim 9.

Claims **20, 30 and 41** are "computer program" and "system" claims analogous to "method" claim 10. Claims 20, 30 and 41 are rejected under same rationale as the rejection of claim 10.

Regarding **Claim 31**, rejection of claim 21 is incorporated and further Akiyama discloses at least one processor comprises at least one of a host processor, a microprocessor, and a microcontroller (Figure 29, processor used in the system of Fig. 29 is a host processor)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian P. Werner can be reached on (571) 272-7401. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

YP
3/05/2007

BRIAN WERNER
SUPERVISORY PATENT EXAMINER